

National Cyber Alert System

Cyber Security Bulletin SB09-131

[Archive](#)

Vulnerability Summary for the Week of May 4, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities (CVSS Score: 7.0 .. 10.0)				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
agtc -- agtc_myshop	AGTC MyShop 3.2b allows remote attackers to bypass authentication and obtain administrative access setting the log_accept cookie to "correcto."	2009-05-06	7.5	CVE-2009-1549 MILWORM
cisco -- wvc54gca	Directory traversal vulnerability in adm/file.cgi on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 allows remote attackers to read arbitrary files via a %2e. (encoded dot dot) or an absolute pathname in the next_file parameter.	2009-05-06	7.8	CVE-2009-1558 XF VUPEN BID MISC
cisco -- wvc54gca	Absolute path traversal vulnerability in adm/file.cgi on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R24 and possibly 1.00R22 allows remote attackers to read arbitrary files via an absolute pathname in the this_file parameter. NOTE: traversal via a .. (dot dot) is probably also possible.	2009-05-06	7.8	CVE-2009-1559 XF VUPEN BID MISC
cisco -- wvc54gc	The Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 stores passwords and wireless-network keys in cleartext in (1) pass_wd.htm and (2) Wsecurity.htm, which allows remote attackers to obtain sensitive information by reading the HTML source code.	2009-05-06	7.8	CVE-2009-1560 VUPEN MISC
	Multiple buffer overflows in Cscope before 15.7a allow			

cscope -- cscope	remote attackers to execute arbitrary code via long strings in input such as (1) source-code tokens and (2) pathnames, related to integer overflows in some cases. NOTE: this issue exists because of an incomplete fix for CVE-2004-2541.	2009-05-05	9.3	CVE-2009-0148 CONFIRM CONFIRM
cscope -- cscope	Multiple stack-based buffer overflows in the putstring function in find.c in Cscope before 15.6 allow user-assisted remote attackers to execute arbitrary code via a long (1) function name or (2) symbol in a source-code file.	2009-05-07	9.3	CVE-2009-1577 CONFIRM CONFIRM CONFIRM
google -- chrome	Heap-based buffer overflow in the ParamTraits::Read function in Google Chrome before 1.0.154.64 allows attackers to leverage renderer access to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to a large bitmap that arrives over the IPC channel.	2009-05-07	9.3	CVE-2009-1441 CONFIRM CONFIRM
hp -- openview_network_node_manager	Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via unknown vectors.	2009-05-05	10.0	CVE-2009-0720 HP HP
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Multiple stack-based buffer overflows in dsagent.exe in the Remote Agent Service in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, and 5.4.0.0 through 5.4.1.96, and the TSM Express client 5.3.3.0 through 5.3.6.4, allow remote attackers to execute arbitrary code via (1) a request packet that is not properly parsed by an unspecified "generic string handling function" or (2) a crafted nodeName in a dicuGetIdentifyRequest request packet, related to the (a) Web GUI and (b) Java GUI.	2009-05-05	10.0	CVE-2008-4828 AIXAPAR CONFIRM
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Buffer overflow in the Web GUI in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17 allows attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors.	2009-05-05	10.0	CVE-2009-1520 AIXAPAR CONFIRM
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Unspecified vulnerability in the Java GUI in the IBM Tivoli Storage Manager (TSM) client 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.5, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17, and the TSM Express client 5.3.3.0 through 5.3.6.5, allows attackers to read or modify arbitrary files via unknown vectors.	2009-05-05	7.5	CVE-2009-1521 AIXAPAR CONFIRM
icewarp -- merak_mail_server	Stack-based buffer overflow in the IceWarpServer.APIObject ActiveX control in api.dll in IceWarp Merak Mail Server 9.4.1 might allow context-dependent attackers to execute arbitrary code via a large value in the second argument to the Base64FileEncode method, as possibly demonstrated by a web application that accepts untrusted input for this method.	2009-05-04	7.5	CVE-2009-1516 BID MILWORM
jbmc-software -- directadmin	CMD_DB in JBMC Software DirectAdmin before 1.334 allows remote authenticated users to gain privileges via shell metacharacters in the name parameter during a restore action.	2009-05-05	8.5	CVE-2009-1525 XF CONFIRM SECUNIA

	a restore action.			OSVDB FULLDISC
jeremy_powers -- lizardware_cms	SQL injection vulnerability in administrator/index.php in Lizardware CMS 0.6.0 and earlier allows remote attackers to execute arbitrary SQL commands via the user.	2009-05-01	7.5	CVE-2008-6787 XF BID MILWoRM
kalptarudemos -- million_dollar_text_links	Million Dollar Text Links 1.0 does not properly restrict administrator access to admin.home.php, which allows remote attackers to bypass intended restrictions and gain privileges via a direct request to admin.home.php after visiting admin.php.	2009-05-07	7.5	CVE-2009-1582 XF BID MILWoRM SECUNIA OSVDB
kalptarudemos -- php_site_lock	index.php in PHP Site Lock 2.0 allows remote attackers to bypass authentication and obtain administrative access by setting the login_id, group_id, login_name, user_id, and user_type cookies to certain values.	2009-05-07	7.5	CVE-2009-1587 XF VUPEN MILWoRM SECUNIA OSVDB
mcafee -- groupshield	McAfee GroupShield for Microsoft Exchange on Exchange Server 2000, and possibly other anti-virus or anti-spam products from McAfee or other vendors, does not scan X- headers for malicious content, which allows remote attackers to bypass virus detection via a crafted message, as demonstrated by a message with an X-Testing header and no message body.	2009-05-05	10.0	CVE-2009-1491 MISC
mitel -- mitel_nupoint_messenger	The server in Mitel NuPoint Messenger R11 and R3 sends usernames and passwords in cleartext to Exchange servers, which allows remote attackers to obtain sensitive information by sniffing the network.	2009-05-07	7.8	CVE-2008-6797 CERT-VN BID MISC
mortbay -- jetty	Directory traversal vulnerability in the HTTP server in Mort Bay Jetty before 6.1.17, and 7.0.0.M2 and earlier 7.x versions, allows remote attackers to access arbitrary files via directory traversal sequences in the URI.	2009-05-05	7.1	CVE-2009-1523 CERT-VN BID CONFIRM SECUNIA CONFIRM
niclor -- vibro-school-cms	SQL injection vulnerability in view_news.php in nicLOR Vibro-School-CMS allows remote attackers to execute arbitrary SQL commands via the nID parameter.	2009-05-07	7.5	CVE-2008-6795 XF BID MILWoRM
phpexplorer -- phphotogallery	Multiple SQL injection vulnerabilities in index.php in phPhotoGallery 0.92 allow remote attackers to execute arbitrary SQL commands via the (1) Username and (2) Password fields. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-07	7.5	CVE-2008-6802 MISC
preprojects -- pre_real_estate_listings	SQL injection vulnerability in manager/login.php in Pre Projects Pre Real Estate Listings allows remote attackers to execute arbitrary SQL commands via the username1 parameter (aka the Admin field or Username field).	2009-05-07	7.5	CVE-2008-6796 XF VUPEN BID MILWoRM

preprojects -- pre_real_estate_listings	Multiple SQL injection vulnerabilities in login.php in Pre Projects Pre Real Estate Listings allow remote attackers to execute arbitrary SQL commands via (1) the us parameter (aka the Username field) or (2) the ps parameter (aka the Password field).	2009-05-07	7.5	CVE-2008-6798 BID MILWoRM
qsix -- blusky_cms	SQL injection vulnerability in index.php in BluSky CMS allows remote attackers to execute arbitrary SQL commands via the news_id parameter in a read action.	2009-05-06	7.5	CVE-2009-1548 MILWoRM
qt-cute -- quickteam	Multiple PHP remote file inclusion vulnerabilities in Qt quickteam 2 allow remote attackers to execute arbitrary PHP code via a URL in the (1) qte_web_path parameter to qte_web.php and the (2) qte_root parameter to bin/qte_init.php.	2009-05-06	7.5	CVE-2009-1551 MILWoRM
sco -- unixware	Unspecified vulnerability in the IGMP driver in SCO Unixware Release 7.1.4 Maintenance Pack 4 allows attackers to cause a denial of service (system panic) via unspecified vectors.	2009-05-06	7.8	CVE-2009-1552 XF BID CONFIRM
sfs_ez_pub -- fsf_ex_pub	SQL injection vulnerability in directory.php in Scripts For Sites (SFS) EZ Pub Site allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-05-07	7.5	CVE-2008-6794 MILWoRM SECUNIA OSVDB
shemes -- grabit	Stack-based buffer overflow in the NZB importer feature in GrabIt 1.7.2 Beta 3 and earlier allows remote attackers to execute arbitrary code via a crafted DTD reference in a DOCTYPE element in an NZB file.	2009-05-07	9.3	CVE-2009-1586 CONFIRM
tufat -- flashchat	connection.php in FlashChat 5.0.8 allows remote attackers to bypass the role filter mechanism and gain administrative privileges by setting the s parmaeter to "7."	2009-05-07	7.5	CVE-2008-6799 XF BID OSVDB SECUNIA MISC BUGTRAQ

[Back to top](#)

Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
beltane -- beltane	Cross-site request forgery (CSRF) vulnerability in Beltane before 2.3.11 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-04	6.8	CVE-2009-1518 SECUNIA OSVDB
branden_robinson -- xvfb-run debian -- debian_linux redhat -- fedora ubuntu -- linux	xvfb-run 1.6.1 in Debian GNU/Linux, Ubuntu, Fedora 10, and possibly other operating systems place the magic cookie (MCOOKIE) on the command line, which allows local users to gain privileges by listing the process and its arguments.	2009-05-06	4.6	CVE-2009-1573 MLIST MLIST CONFIRM
cgi_rescue -- cgi_rescue_minibbs	Cross-site scripting (XSS) vulnerability in CGI RESCUE MiniBBS 8t before 8.95t, 8 before 8.95, 9 before 9.08, and 10 before 10.32 allows remote attackers to inject	2009-05-08	4.3	CVE-2009-1588 JVNDB

	arbitrary web script or HTML via unspecified vectors.			JVN
christos_zoulas -- file	Heap-based buffer overflow in the <code>cdf_read_sat</code> function in <code>src/cdf.c</code> in Christos Zoulas file 5.00 allows user-assisted remote attackers to execute arbitrary code via a crafted compound document file, as demonstrated by a <code>.msi</code> , <code>.doc</code> , or <code>.mpp</code> file. NOTE: some of these details are obtained from third party information.	2009-05-04	6.8	CVE-2009-1515 BID OSVDB SECUNIA MISC MISC CONFIRM
cisco -- firmware	The Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 sends configuration data in response to a Setup Wizard remote-management command, which allows remote attackers to obtain sensitive information such as passwords by reading the <code>SetupWizard.exe</code> process memory, a related issue to CVE-2008-4390.	2009-05-06	5.0	CVE-2009-1555 VUPEN MISC SECUNIA
cisco -- wvc54gca	Multiple cross-site scripting (XSS) vulnerabilities on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 allow remote attackers to inject arbitrary web script or HTML via the <code>next_file</code> parameter to (1) <code>main.cgi</code> , (2) <code>img/main.cgi</code> , or (3) <code>adm/file.cgi</code> ; or (4) the <code>this_file</code> parameter to <code>adm/file.cgi</code> .	2009-05-06	4.3	CVE-2009-1557 XF VUPEN MISC SECUNIA
cisco -- wrt54gc	Cross-site request forgery (CSRF) vulnerability in <code>administration.cgi</code> on the Cisco Linksys WRT54GC router with firmware 1.05.7 allows remote attackers to hijack the intranet connectivity of arbitrary users for requests that change the administrator password via the <code>sysPasswd</code> and <code>sysConfirmPasswd</code> parameters.	2009-05-06	6.8	CVE-2009-1561 VUPEN BID MISC SECUNIA MISC BUGTRAQ
dflabs -- ptk	The <code>get_file_type</code> function in <code>lib/file_content.php</code> in DFLabs PTK 0.1, 0.2, and 1.0 allows remote attackers to execute arbitrary commands via shell metacharacters after an <code>arg1=</code> sequence in a filename within a forensic image.	2009-05-07	6.8	CVE-2008-6793 VUPEN
drupal -- drupal	Cross-site scripting (XSS) vulnerability in Drupal 5.x before 5.17 and 6.x before 6.11, as used in <code>vbDrupal</code> before 5.17.0, allows remote attackers to inject arbitrary web script or HTML via crafted UTF-8 byte sequences before the <code>Content-Type</code> meta tag, which are treated as UTF-7 by Internet Explorer 6 and 7.	2009-05-06	4.3	CVE-2009-1575 VUPEN CONFIRM OSVDB CONFIRM
drupal -- drupal	Unspecified vulnerability in Drupal 5.x before 5.17 and 6.x before 6.11, as used in <code>vbDrupal</code> before 5.17.0, allows user-assisted remote attackers to obtain sensitive information by tricking victims into visiting the front page of the site with a crafted URL and causing form data to be sent to an attacker-controlled site, possibly related to multiple / (slash) characters that are not properly handled by <code>includes/bootstrap.inc</code> , as demonstrated using the search box. NOTE: this vulnerability can be leveraged to conduct cross-site request forgery (CSRF) attacks.	2009-05-06	4.3	CVE-2009-1576 FEDORA FEDORA CONFIRM CONFIRM MISC
google -- chrome	Google Chrome 1.0.154.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a <code>throw</code> statement with a long exception value.	2009-05-04	5.0	CVE-2009-1514 BID MILWORM

google -- chrome	Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.	2009-05-07	6.8	CVE-2009-1442 CONFIRM
ibm -- tivoli_storage_manager_client	The IBM Tivoli Storage Manager (TSM) client 5.5.0.0 through 5.5.1.17 on AIX and Windows, when SSL is used, allows remote attackers to conduct unspecified man-in-the-middle attacks and read arbitrary files via unknown vectors.	2009-05-05	5.0	CVE-2009-1522 AIXAPAR CONFIRM
icewarp -- email_server icewarp -- webmail_server	Multiple cross-site scripting (XSS) vulnerabilities in IceWarp eMail Server and WebMail Server before 9.4.2 allow remote attackers to inject arbitrary web script or HTML via (1) the body of a message, related to the email view and incorrect HTML filtering in the cleanHTML function in server/inc/tools.php; or the (2) title, (3) link, or (4) description element in an RSS feed, related to the getHTML function in server/inc/rss/item.php.	2009-05-05	4.3	CVE-2009-1467 MISC
icewarp -- email_server icewarp -- webmail_server	Multiple SQL injection vulnerabilities in the search form in server/webmail.php in the Groupware component in IceWarp eMail Server and WebMail Server before 9.4.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) sql and (2) order_by elements in an XML search query.	2009-05-05	6.5	CVE-2009-1468 BID BUGTRAQ MISC
icewarp -- email_server icewarp -- webmail_server	CRLF injection vulnerability in the Forgot Password implementation in server/webmail.php in IceWarp eMail Server and WebMail Server before 9.4.2 makes it easier for remote attackers to trick a user into disclosing credentials via CRLF sequences preceding a Reply-To header in the subject element of an XML document, as demonstrated by triggering an e-mail message from the server that contains a user's correct credentials, and requests that the user compose a reply that includes this message.	2009-05-05	4.3	CVE-2009-1469 BUGTRAQ MISC
ipsec-tools -- ipsec-tools	racoon/isakmp_frag.c in ipsec-tools before 0.7.2 allows remote attackers to cause a denial of service (crash) via crafted fragmented packets without a payload, which triggers a NULL pointer dereference.	2009-05-06	5.0	CVE-2009-1574 CONFIRM MLIST MLIST
jbmc-software -- directadmin	JBMC Software DirectAdmin before 1.334 allows local users to create or overwrite any file via a symlink attack on an arbitrary file in a certain temporary directory, related to a request for this temporary file in the PATH_INFO to the CMD_DB script during a backup action.	2009-05-05	6.9	CVE-2009-1526 CONFIRM SECUNIA OSVDB FULLDISC
klever -- pumpkin	PumpKIN TFTP Server 2.7.2.0 allows remote attackers to cause a denial of service via a write request with a long mode field.	2009-05-04	5.0	CVE-2008-6791 XF BID MILWoRM
konstanty_bialkowski -- libmodplug	Buffer overflow in the PATinst function in src/load_pat.cpp in libmodplug before 0.8.7 allows user-assisted remote attackers to cause a denial of service and possibly execute arbitrary code via a long instrument name.	2009-05-04	6.8	CVE-2009-1513 VUPEN BID CONFIRM CONFIRM

				CONFIRM
linux -- kernel	The selinux_ip_postroute_iptables_compat function in security/selinux/hooks.c in the SELinux subsystem in the Linux kernel before 2.6.27.22, and 2.6.28.x before 2.6.28.10, when compat_net is enabled, omits calls to avc_has_perm for the (1) node and (2) port, which allows local users to bypass intended restrictions on network traffic. NOTE: this was incorrectly reported as an issue fixed in 2.6.27.21.	2009-05-05	4.4	CVE-2009-1184 CONFIRM
linux -- kernel	Race condition in the ptrace_attach function in kernel/ptrace.c in the Linux kernel before 2.6.30-rc4 allows local users to gain privileges via a PTRACE_ATTACH ptrace call during an exec system call that is launching a setuid application, related to locking an incorrect cred_exec_mutex object.	2009-05-05	6.9	CVE-2009-1527 VUPEN CONFIRM
minddezn -- photo_gallery	SQL injection vulnerability in MindDezign Photo Gallery 2.2, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter in an info action to index.php.	2009-05-04	5.1	CVE-2008-6788 XF BID MILWoRM SECUNIA OSVDB
minddezn -- photo_gallery	SQL injection vulnerability in MindDezign Photo Gallery 2.2 allows remote attackers to execute arbitrary SQL commands via the username parameter in a login action to the admin module in index.php, a different vector than CVE-2008-6788.	2009-05-04	5.1	CVE-2008-6789 XF MILWoRM SECUNIA
minddezn -- photo_gallery	The admin module in MindDezign Photo Gallery 2.2 allows remote attackers to add administrative users and gain privileges via a modified username parameter in an edit account action to index.php.	2009-05-04	5.1	CVE-2008-6790 XF BID MILWoRM
mortbay -- jetty	Cross-site scripting (XSS) vulnerability in Mort Bay Jetty before 6.1.17 allows remote attackers to inject arbitrary web script or HTML via a directory listing request containing a ; (semicolon) character.	2009-05-05	4.3	CVE-2009-1524 CONFIRM
pecio-cms -- pecio_cms	Directory traversal vulnerability in index.php in Pecio CMS 1.1.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the language parameter.	2009-05-04	5.0	CVE-2009-1519 MILWoRM
quagga -- quagga_routing_software_suite	The BGP daemon (bgpd) in Quagga 0.99.11 and earlier allows remote attackers to cause a denial of service (crash) via an AS path containing ASN elements whose string representation is longer than expected, which triggers an assert error.	2009-05-06	5.0	CVE-2009-1572 DEBIAN MLIST CONFIRM
ro20 -- tematres	Multiple cross-site scripting (XSS) vulnerabilities in TemaTres 1.0.3 and 1.031 allow remote attackers to inject arbitrary web script or HTML via the (1) search form; (2) _expresion_de_búsqueda, (3) letra, (4) estado_id, and (5) tema parameters to index.php; the (6) PATH_INFO to index.php; and the (7) y, (8) ord, and (9) m parameters to sobre.php.	2009-05-07	4.3	CVE-2009-1583 BID BUGTRAQ MILWoRM SECUNIA
ro20 -- tematres	Multiple SQL injection vulnerabilities in TemaTres 1.0.3 and 1.031, when magic_quotes_gpc is disabled, allow remote attackers or remote authenticated users to execute arbitrary SQL commands via the (1) mail, (2) password, and (3) letra parameters to index.php; (4) y	2009-05-07	6.0	CVE-2009-1584 BID BUGTRAQ BUGTRAQ

	and (5) m parameters to sobre.php; and the (6) dcTema, (7) madsTema, (8) zthesTema, (9) skosTema, and (10) xtmTema parameters to xml.php.			MILWoRM MILWoRM SECUNIA
ro20 -- tematres	Multiple SQL injection vulnerabilities in TemaTres 1.031, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) id_correo_electronico and (2) id_password parameters to login.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-07	4.4	CVE-2009-1585 SECUNIA
samba -- samba	Race condition in the winbind daemon (aka winbindd) in Samba before 3.0.32 allows attackers to cause a denial of service (crash) via unspecified vectors related to an "unresponsive" child process.	2009-05-07	4.3	CVE-2008-6800 CONFIRM
sendmail -- sendmail	Heap-based buffer overflow in Sendmail before 8.13.2 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long X- header, as demonstrated by an X-Testing header.	2009-05-05	5.0	CVE-2009-1490 CONFIRM
sun -- glassfish_enterprise_server	Multiple cross-site scripting (XSS) vulnerabilities in the Admin Console in Sun GlassFish Enterprise Server 2.1 allow remote attackers to inject arbitrary web script or HTML via the query string to (1) applications/applications.jsf, (2) configuration/configuration.jsf, (3) customMBeans/customMBeans.jsf, (4) resourceNode/resources.jsf, (5) sysnet/registration.jsf, or (6) webService/webServicesGeneral.jsf; or the name parameter to (7) configuration/auditModuleEdit.jsf, (8) configuration/httpListenerEdit.jsf, or (9) resourceNode/jdbcResourceEdit.jsf.	2009-05-06	4.3	CVE-2009-1553 MLIST MLIST MLIST
sun -- woodstock	Cross-site scripting (XSS) vulnerability in ThemeServlet.java in Sun Woodstock 4.2, as used in Sun GlassFish Enterprise Server and other products, allows remote attackers to inject arbitrary web script or HTML via a UTF-7 string in the PATH_INFO, which is displayed on the 404 error page, as demonstrated by the PATH_INFO to theme/META-INF.	2009-05-06	4.3	CVE-2009-1554 MLIST
symantec -- norton_ghost	Multiple insecure method vulnerabilities in the Symantec.EasySetup.1 ActiveX control in EasySetupInt.dll 14.0.4.30167 in the EasySetup wizard in Symantec Norton Ghost 14.0 allow remote attackers to cause a denial of service (browser crash) and possibly execute arbitrary code via unspecified input to the (1) GetBackupLocationPath, (2) CallUninstall, (3) SetupDeleteVolume, (4) CanUseEasySetup, (5) CallAddInitialProtection, and (6) CallTour methods.	2009-05-04	4.3	CVE-2009-1517 XF MISC SECTRACK BID MILWoRM
ubuntu -- linux	system-tools-backends before 2.6.0-1ubuntu1.1 in Ubuntu 8.10, as used by "Users and Groups" in GNOME System Tools, hashes account passwords with 3DES and consequently limits effective password lengths to eight characters, which makes it easier for context-dependent attackers to successfully conduct brute-force password attacks.	2009-05-07	5.0	CVE-2008-6792 CONFIRM UBUNTU SECUNIA OSVDB
vivvo -- vivvo	Cross-site request forgery (CSRF) vulnerability in Vivvo CMS before 4.0.4 allows remote attackers to hijack the	2009-05-	4.4	CVE-2008-6801 XF

vivvo -- vivvo	authentication of unspecified victims via unknown vectors.	07	4.4	CONFIRM OSVDB SECUNIA
zakkis -- abc_advertise	Zakkis Technology ABC Advertise 1.0 does not properly restrict access to admin.inc.php, which allows remote attackers to obtain the administrator login name and password via a direct request.	2009-05-06	5.0	CVE-2009-1550 XF MILWORM

[Back to top](#)

Low Vulnerabilities (CVSS Score: 0.0 .. 3.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firmware	img/main.cgi on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 allows remote authenticated users to read arbitrary files in img/ via a filename in the next_file parameter, as demonstrated by reading .htpasswd to obtain the admin password, a different vulnerability than CVE-2004-2507.	2009-05-06	3.5	CVE-2009-1556 VUPEN MISC SECUNIA

[Back to top](#)

Last updated May 11, 2009

